

CLAIMS

What is claimed is:

1. A method (200) of verifying the integrity of software resident in a remote device in a network operated by a host, comprising the steps of:
 - providing a copy of the memory associated with said remote device to said host;
 - identifying, by said host, a subset of said memory associated with remote device;
 - inserting, by said host, a random seed at a predetermined address within said memory subset;
 - performing (202), by said host, a hash function on said memory subset containing said seed;
 - determining a host hash value as a result of said performing step;
 - transmitting (204) said seed and indicia of said memory subset from said host to said remote device;
 - inserting, by said remote device, said hash function on said memory subset containing said seed;
 - determining (208), by said remote device a remote hash value as a result of said executing step;
 - transmitting (210) said remote hash value from said remote device to said host; and
 - comparing (212), by said host, said host hash value to said remote hash value.
2. The method of claim 1, further comprising the step of determining a range that defines the subset of said memory
3. The method of claim 2, wherein the subset of code corresponds to code between a beginning address and an ending address, associated within a sector memory.
4. The method of claim 1, further comprising the step of identifying an intermediary address (112).